BOBBY JINDAL
GOVERNOR

State of Louisiana
Governor's Office of Homeland Security
and
Emergency Preparedness

KEVIN DAVIS
DIRECTOR

PERSONALLY IDENTIFIABLE INFORMATION (PII)
Policy Number: GEN-0013

Issue Date: May 27, 2015
Revised Date:

Approval:

Kevin Davis, Director

I. POLICY

Pursuant to 2 CFR 200.303 (e), in its capacity as a non-Federal entity managing Federal awards, the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) is required to establish and maintain effective internal controls to safeguard protected personally identifiable information (PII) and other information which the Federal entity or the non-Federal entity considers sensitive.

II. PURPOSE

This policy establishes the procedures to protect PII for the Federal grant related and other programs administered by GOHSEP.

III. APPLICABILITY

This policy applies to all employees of the GOHSEP and extends to anyone with whom GOHSEP does business with including, but not limited to, vendors and contractors.

IV. DEFINITIONS

A. **Personally Identifiable Information (PII)**: : Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an

individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. When approval is granted to take sensitive information away from the office, the employee must adhere to the GOHSEP security policies.

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.[1]

B. **Protected Personally Identifiable Information (Protected PII)**: *Protected PII* means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.[2]

C. **Minimum Necessary**: *Minimum Necessary* is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.[3]

[1] 2 CFR 200.79
[2] 2 CFR 200.82
[3] 2 CFR 200.

V. PROCEDURES

A. Employees are reminded that safeguarding sensitive information is a critical responsibility that must be taken seriously at all times. Internal policy specifies the following security policies for the protection of PII and other sensitive data: It is the responsibility of the individual user to protect data to which they have access. Users must adhere to the rules of behavior defined in applicable Systems Security Plans, and agency guidance.

B. Employees having access to personal information shall respect the confidentiality of such information, and refrain from any conduct that would indicate a careless or negligent attitude toward such information. Employees also shall avoid office gossip and should not permit any unauthorized viewing of records contained in a GOHSEP system of records. Only individuals who have a "need to know" in their official capacity shall have access to such systems of records.

C. The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because employees and contractors may have access to personal identifiable information concerning individuals and other sensitive data, we have a special responsibility to protect that information from loss and misuse.

D. As a general rule, all PII contained in grant programs are to be protected and not released to the public. See paragraph VII for exceptions.

E. With these responsibilities contractors should ensure that their employees:

   a. Safeguard information to which their employees have access at all times.

   b. Obtain a management's written approval prior to taking any sensitive information away from the office. The manager's approval must identify the business necessity for removing such information from the agency.

VI. CATEGORIZATION OF INFORMATION

A. Federal grant programs that **do not** contain any PII as defined by federal regulation is releasable to the public pursuant to the Louisiana Public Records Law, Louisiana Revised Statute 44:1, et seq.

B. Federal grant programs that **do** contain PII as defined by federal regulation, and/or has been determined by the Louisiana courts to be **protected** information should not be disclosed to the public.

VII. EXCEPTIONS

Individual requests for exceptions to the policy must be submitted with specific and compelling justification to the Appointing Authority.

VIII. VIOLATIONS

Violations of this policy resulting in unauthorized disclosure of protected personally identifiably information may subject individuals to legal and/or disciplinary action, up to and including termination of employment.

IX. QUESTIONS

Questions regarding this policy should be directed to your immediate supervisor.